UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,320	10/16/2003	Frank J. Hammond II	413130	8493

30955 7590 03/26/2007

LATHROP & GAGE LC
4845 PEARL EAST CIRCLE
SUITE 300
BOULDER, CO 80301

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/687,320	HAMMOND ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 October 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-13 are pending and have been examined.

Information Disclosure Statement

2. It is noted that no Information Disclosure Statement has been filed on this application.

Drawings

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 12 (fig, 1), 32 (fig. 2), 80 (fig. 3). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

This is not intended to be a complete list of such reference characters.

Specification

4. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: claim 5's "creating a prover agent application on the client".

Claim Objections

5. Claim 11 is objected to because of the following informalities: "further comprising **periodically and distributing**". Appropriate correction is required.

6. Claim 11 is objected to because of the following informalities: "LAN" must be spelled out. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claim 5 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. It is not clear what the metes and bounds of "creating a prover / verifier agent application on the client / host" are intended to be.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Le et al. (US Patent Application Publication 2004/0008845, hereinafter Le).

Regarding claim 1, Le teaches

- a method of non-centralized zero-knowledge authentication for a computer network **(abstract)**, comprising steps of:
- establishing a first computer having a first authentication agent and a first prover agent on the computer network **(paragraphs 25-30)**;
- detecting a first authentication request over the computer network from a second computer having a second prover agent **(paragraphs 30-33)**;
- authenticating the second prover agent through a zero-knowledge identification protocol **(paragraphs 30-33)**; and
- promoting the second computer with a second authentication agent to perform authentication for the computer network **(paragraphs 30-33)**.

Regarding claim 5, Le teaches

- a method of protecting a host from unauthorized client access over a network **(abstract)**, comprising the steps of:
- creating a prover agent application on the client **(paragraphs 25-30)**;
- creating a verifier agent application on the host **(paragraphs 25-30)**;
- creating a trusted source application to generate and publish encrypted values of a secret and product of first and second large prime numbers; reading the encrypted values for the secret and product, by the prover and verifier from the trusted source **(paragraphs 69-89)**;
- decrypting the secret, by the prover and verifier; decrypting the product, by the prover and verifier **(paragraphs 69-89)**; and
- performing a plurality of verification dialog between the prover and verifier, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access when the prover fails to demonstrate knowledge of the secret and product and granted access when the client succeeds in demonstrating knowledge of the secret and product **(paragraphs 141-170)**.

Regarding claim 8, Le teaches

- a system of non-centralized zero-knowledge authentication for a computer network **(abstract)**, comprising:

- two or more computers establishing the computer network, each of the computers containing an authentication agent, secret and prover agent **(paragraphs 41-49)**; and
- a requesting computer having a prover agent, for requesting access to the computer network, wherein the prover agent of the requesting computer and one of the authentication agents of the two or more computers engaging in a zero-knowledge authentication protocol, and wherein the requesting computer operates with an authentication agent on the computer network when the requesting computer is authenticated through the zero-knowledge authentication protocol **(paragraphs 25-33 and 69-89)**.

Regarding claim 13, Le teaches

- a software product comprising instructions, stored on computer-readable media, wherein the instructions, when executed by a computer, perform steps for non-centralized zero-knowledge authentication for a computer network **(abstract)**, comprising:
- instructions for establishing a first computer having a first authentication agent and a first prover agent on the computer network **(paragraphs 25-30)**;
- instructions for detecting a first authentication request over the computer network from a second computer having a second prover agent **(paragraphs 30-33)**;

- instructions for authenticating the second prover agent through a zero-knowledge identification protocol **(paragraphs 30-33)**; and
- instructions for promoting the second computer with a second authentication agent to perform authentication for the computer network **(paragraphs 30-33)**.

Regarding claim 2, Le teaches periodically and distributing a new secret to the first and second authentication agents **(paragraphs 112-126)**.

Regarding claim 3, Le teaches

- detecting a second authentication request over the computer network from a third computer having a third prover agent **(paragraphs 30-33)**;
- authenticating the third prover agent through a zero-knowledge identification protocol with the second authentication agent **(paragraphs 30-33)**; and
- promoting the third computer with a third authentication agent to perform authentication for the computer network **(paragraphs 30-33)**.

Regarding claim 4, Le teaches

- periodically publishing encrypted numbers for the zero-knowledge identification protocol **(paragraphs 112-126)**, including the steps of:
- generating a first and second large prime numbers **(paragraphs 140-143)**;
- calculating a product of the first and second large prime numbers **(paragraphs 140-143)**;

- generating a secret to have a value relatively prime to the product, greater than zero and less than the product **(paragraphs 147-157)**;
- encrypting the product; encrypting the secret **(paragraphs 151-159)**; and
- publishing encrypted values of the secret and product **(paragraphs 142-151)**.

Regarding claim 6, Le teaches

- wherein the steps of decrypting the secret and product further utilize previous values of the secret and product as operators in the modulus inverse operations **(paragraphs 69-89, 143-157)**.

Regarding claim 7, Le teaches

- creating a first agent to be authenticated, the first agent having values for s, n and t, s being the secret, n being the product, and t being a size of an answer set **(paragraphs 142-144)**;
- creating a second agent to authenticate the first agent, the second agent having values for s, n, and t **(paragraphs 142-144)**;
- generating r as a random number generated by the first agent **(paragraphs 151-156)**;
- calculating x by the first agent, r being raised to power of t modulus n **(paragraphs 151-156)**;
- sending x from the first agent to the second agent **(paragraphs 151-156)**;

- calculating b by the second agent, b being further defined as a member of set of integers from zero through t-1; sending b from the second agent to the first agent **(paragraphs 151-156)**;
- calculating y by the first agent, y being a product of r*s raised to power of b **(paragraphs 151-156)**;
- sending y from the first agent to the second agent **(paragraph 154)**; and
- determining authentication of the first agent, by determining equivalence of a first equation to a second equation, if y is not equal to zero, first equation is y^t mod n and second equation is (xv^b) mod n **(paragraphs 151-156)**.

Regarding claim 9, Le teaches a trusted source for periodically generating a new secret for the authentication agents of computers on the network **(paragraphs 112-126)**.

Regarding claim 10, Le teaches the requesting computer comprising a cell phone **(paragraphs 127-133 and 165-173)**.

Regarding claim 11, Le teaches the computer network comprising one or more of the Internet, LAN, communications link, and a wireless network **(paragraph 172)**.

Regarding claim 12, Le teaches the authentication agents and prover agents being installed on each of the computers through common software **(paragraphs 142-147)**.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

12. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

13. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DGC

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

3/21/07